

This record is a partial extract of the original cable. The full text of the original cable is not available.

UNCLAS SECTION 01 OF 02 ABUJA 000484

SIPDIS

STATE FOR IIP/T/TP PEN AGNEW AND AF/PD

E.O. 12958: N/A

TAGS: [OIIP](#) [KPAO](#) [NI](#)

SUBJECT: NIGERIA AND GTC PROPOSAL

REFTEL: STATE 033002

1. Overview: The U.S. Mission in Nigeria proposes that GTC and the Mission partner with NITDA (National Information Technology Development Agency) to combat cybercrime, a well-known threat both inside and outside of Nigeria through 419 emails. Increasingly, the Government of Nigeria is concerned about the potential destabilizing effect of cybercrime to Nigeria's banking and commercial sectors. As a basis for combating cybercrime, Nigeria's criminal laws must conform to the newly emergent threat. Current laws did not foresee information and communications technology (ICT) and its possible criminal use. While Nigeria's private sector in ICT has generated immense foreign and domestic investment in this key sector, there are no laws or enforcement institutions created specifically to prohibit and enforce actions directed at these ICT infrastructures.
2. In addition, no country parallels Nigeria in electronically generated 419 scams. While the Nigerian Economic and Financial Crimes Commission (EFCC) is statutorily empowered to enforce Nigeria's financial crimes laws, under which 419 falls, Nigeria's laws only contemplate the traditional non-ICT environment. Internet-based 419 scams are not legally covered at present. Further, if a criminal is apprehended using cyber-tracking means, evidence of his/her activities may be inadmissible in Nigerian courts as the current laws are mute on this subject. A recent judgment by the Kaduna State Court of Appeals denied evidential admissibility of a computer-generated accounts statement on the grounds that the statement did not meet the definition of a "book" as stipulated under the Nigerian Evidence Act.
3. Recently, the GON - at NITDA's urging - established a Presidential Committee on Cybercrime to examine the need for cybercrime laws in Nigeria and what mechanism is best suited for enforcing such laws. The Committee's recommendations included the drafting of new legislation dealing with cybercrime, formation of a Nigerian Cybercrime Working Group (NCWG) to do public education and gain National Assembly support for such legislation, and the establishment of a separate agency for enforcing new cybercrime laws. Two of the three recommendations have been carried out; law enforcement elements and the EFCC have resisted the establishment of a separate enforcement agency for cybercrime. The NCWG has drafted a Cybercrime Act, but it has not yet been reviewed within the GON nor submitted to the National Assembly. Relevant sectors of the GON (primarily judicial, law enforcement, and intelligence officials) as well as the National Assembly will require technical assistance to understand the draft law and its ramifications, as well as how it articulates with traditional criminal law. Private sector consultation and training is also necessary so that telecommunications officials and related service providers, Internet Service Providers (ISPs) and cybercafe owners are also adequately informed. The NCWG is inadequately staffed to provide such technical training.
4. Project Description: The Mission seeks USGTC professional(s) to assist the NCWG to brief GON stakeholders on the draft Cybercrime Act (Phase 1), and once approved, brief National Assembly legislators on the Act (Phase 2) to ensure its passage. USGTC partner(s) should be familiar with cybercrime laws in the United States, Europe, and the developing world, and be able to brief legislative bills concerning ICT to non-experts. A combination of legal expertise and computer/ICT skills is desired. Post would also want the professional(s) to work with the NCWG to develop an appropriate public education strategy for explaining the issue of cybercrime and the enacted legislation to Nigeria's ICT community and the media (Phase 3). As part of Phase 3, we would also ask that USGTC investigate if any of the current anti-spam software might be used to assist in identifying and screening out 419 emails - such information and software would be useful to share with stakeholders here.

15. Timeframe: Post would anticipate conducting the Phase 1 training in the last quarter of FY 04, and the Phase 2 training in the first quarter of FY 05. Phase 3 would take place during FY 05.

16. Project Purpose/MPP Goals: Assisting the GON in the area of cybercrime falls under International Crime.

17. Primary Contact: Primary contact for the proposal is Margaret McKean, Information Officer, U.S. Embassy Abuja, 234-9-523-2018, McKeanMB@state.gov

18. Audiences: The audiences for the proposal are relevant stakeholders within the GON whose offices will be concerned with cybercrime and enacted legislation, members of the National Assembly who will debate and vote the draft Cybercrime Act into law, and members of the public - particularly those sectors most concerned with ICT. NITDA is the GON's chief agency for ICT issues, and has strong support from President Obasanjo.

19. Cost Sharing: PAS does not have 04 funds to contribute to this project; we may have limited funds for local per diem and travel in FY 05, but another continuing resolution would likely negate this probability. INL has some funding for cybercrime, which is primarily slated for law enforcement training and assistance. The USGTC proposal is meant to complement INL initiatives; however, INL funding will not be able to contribute to the current proposal.

110. Follow-on: Through the EDDI initiative, the Mission has already established a strong partnership with NITDA; INL has a broad assistance program with law enforcement and security agencies in Nigeria, and USAID has a multi-year project with the court system. These partnerships will dovetail in the Mission's efforts to assist the GON deal with cybercrime, and particularly Internet-based 419 scams.

111. Language requirements: English.

ROBERTS